

Author index volume 226 (1999)

(The issue number is given in front of the page numbers)

- Adleman, L.M., J. DeMarrais and M.-D. Huang, A subexponential algorithm for discrete logarithms over hyperelliptic curves of large genus over $\text{GF}(q)$ (1-2) 7- 18
- Chen, S., *see* R. Tao (1-2) 143-172
- Chua, S.K., K. H. Leung and S. Ling, Attack on RSA-type cryptosystems based on singular cubic curves over $\mathbb{Z}/n\mathbb{Z}$ (1-2) 19- 27
- Cusick, T.W., The Ajtai Random class of lattices (1-2) 29- 36
- DeMarrais, J., *see* L.M. Adleman (1-2) 7- 18
- Ding, C., Preface (1-2) 1- 2
- Feng, D., Three characterizations of correlation-immune functions over rings \mathbb{Z}_N (1-2) 37- 43
- Gollmann, D., Dual bases and bit-serial multiplication in \mathbb{F}_{q^r} (1-2) 45- 59
- Herrigel, A., *see* J. Ó Ruanaidh (1-2) 117-142
- Huang, M.-D., *see* L.M. Adleman (1-2) 7- 18
- Imai, H., *see* Y. Zheng (1-2) 207-223
- Jajodia, S., *see* C. Zhang (1-2) 185-206
- Karhumäki, J., A short biography of Arto Salomaa (1-2) 3- 5
- Klapper, A. and J. Xu, Algebraic feedback shift registers (1-2) 61- 92
- Lam, K.-Y., *see* C. Zhang (1-2) 185-206
- Leung, K.H., *see* S.K. Chua (1-2) 19- 27
- Ling, S., *see* S.K. Chua (1-2) 19- 27
- Mu, Y., *see* V. Varadharajan (1-2) 173-184
- Nguyen, K.Q., *see* V. Varadharajan (1-2) 173-184
- Niederreiter, H. and M. Vielhaber, An algorithm for shifted continued fraction expansions in parallel linear time (1-2) 93-104
- Niemi, V. and A. Renvall, Efficient voting with no selling of votes (1-2) 105-116
- Ó Ruanaidh, J., H. Petersen, A. Herrigel, S. Pereira and T. Pun, Cryptographic copyright protection for digital images based on watermarking techniques (1-2) 117-142
- Pereira, S., *see* J. Ó Ruanaidh (1-2) 117-142
- Petersen, H., *see* J. Ó Ruanaidh (1-2) 117-142
- Pun, T., *see* J. Ó Ruanaidh (1-2) 117-142
- Renvall, A., *see* V. Niemi (1-2) 105-116
- Tao, R. and Chen, S., On finite automaton public-key cryptosystem (1-2) 143-172
- Varadharajan, V., K.Q. Nguyen, and Y. Mu, On the design of efficient RSA-based off-line electronic cash schemes (1-2) 173-184
- Vielhaber, M., *see* H. Niederreiter (1-2) 93-104
- Xu, J., *see* A. Klapper (1-2) 61- 92
- Zhang, X.-M., *see* Y. Zheng (1-2) 207-223
- Zhang, C., K.-Y. Lam and S. Jajodia, Scalable threshold closure (1-2) 185-206
- Zheng, Y., Zhang, X.-M. and Imai, H., Restriction, terms and nonlinearity of Boolean functions (1-2) 207-223